Software Engineering Institute
Carnegie Mellon University

1992 CERT Advisories

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 CA-1992-01: NeXTstep Configuration Vulnerability

Original issue date: January 20, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a vulnerability in release 2 of NeXTstep's NetInfo default configuration. This vulnerability will be corrected in future versions of NeXTstep.

I. Description

By default, a NetInfo server process will provide information to any machine that requests it.

II. Impact

Remote users can gain unauthorized access to the network's administrative information such as the passwd file.

III. Solution

Ensure that the trusted_networks property of each NetInfo domain's root NetInfo directory is set correctly, so that only those systems which should be obtaining information from NetInfo are granted access. The value for the trusted_networks property should be the network numbers of the networks the server should trust.

Note that improperly setting trusted_networks can render your network unusable.

Consult Chapter 16, "Security", of the *NeXT Network and System Administration* manual for release 2 for details on setting the trusted_networks property of the root NetInfo directory.

The CERT/CC wishes to thank NeXT Computer, Inc. for their cooperation in documenting and publicizing this security vulnerability.

This document is available from: http://www. cert.org/advisories/CA-1992-01.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

Revision History

```
September 19,1997  Attached copyright statement
```

2 CA-1992-02: Michelangelo PC Virus Warning

Original issue date: February 6, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning a personal computer virus known as Michelangelo. The virus affects IBM PCs and compatibles. A description of the virus, along with suggested countermeasures, is presented below.

I. Description

The Michelangelo virus is a computer virus that affects PCs running MS-DOS (and PC-DOS, DR-DOS, etc.) versions 2.xx and higher. Note, however, that although the virus can only execute on PCs running these versions of DOS, it can infect and damage PC hard disks containing other PC operating systems including UNIX, OS/2, and Novell. Thus, booting an infected DOS floppy disk on a PC that has, for example, UNIX on the hard disk would infect the hard disk and would probably prevent the UNIX disk from booting. The virus infects floppy disk boot sectors and hard disk master boot records (MBRs). When the user boots from an infected floppy disk, the virus installs itself in memory and infects the partition table of the first hard disk (if found). Once the virus is installed, it will infect any floppy disk that the user accesses.

Some possible, though not conclusive, symptoms of the Michelangelo virus include a reduction in free/total memory by 2048 bytes, and some floppy disks that become unusable or display "odd" graphic characters during "DIR" commands. Additionally, integrity management products should report that the MBR has been altered.

Note that the Michelangelo virus does not display any messages on the PC screen at any time.

II. Impact

The Michelangelo virus triggers on any March 6. On that date, the virus overwrites critical system data, including boot and file allocation table (FAT) records, on the boot disk (floppy or hard), rendering the disk unusable. Recovering user data from a disk damaged by the Michelangelo virus will be very difficult.

III. Solution

Many versions of anti-virus software released after approximately October 1991 will detect and/or remove the Michelangelo virus. This includes numerous commercial, shareware, and freeware software packages. Since this virus was first detected around the middle of 1991 (after March 6, 1991), it is crucial to use current versions of these products, particularly those products that search systems for known viruses.

The CERT/CC has not formally reviewed, evaluated, or endorsed any of the anti-virus products. While some older anti-virus products may detect this virus, the CERT/CC strongly suggests that sites verify with their anti-virus product vendors that their product will detect and eradicate the Michelangelo virus.

The CERT/CC advises that all sites test for the presence of this virus before March 6, which is the trigger date. If an infection is discovered, it is essential that the user examine all floppy disks that may have come in contact with an infected machine.

As always, the CERT/CC strongly urges all sites to maintain good backup procedures.

The CERT/CC wishes to thank for their assistance: Mr. Christoph Fischer of the Micro-BIT Virus Center (Germany), Dr. Klaus Brunnstein of the Virus Test Center (Germany), Mr. A. Padgett Peterson, P.E., of the Technical Computing Center at Martin-Marietta Corp., and Mr. Steve R. White of IBM's Thomas J. Watson Research Center.

This document is available from: http://www. cert.org/advisories/CA-1992-02.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

3 CA-1992-03: Internet Intruder Activity

Internet Intruder Activity

Original issue date: February 17,1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information regarding a significant intrusion incident on the Internet. Systems administrators should be aware that many systems on the Internet have been compromised due to this activity. To identify whether your systems have been affected by the activity we recommend that all system administrators check for the signs of intrusion detailed in this advisory.

This advisory describes the activities that have been identified as part of this particular incident. This does not address the possibility that systems may have been compromised due to other, unrelated intrusion activity.

I. Description

The intruders gained initial access to a host by discovering a password for a user account on the system. They then attempted to become root on the compromised system.

II. Impact

Having gained root access on a system, the intruders installed trojan binaries that captured account information for both local and remote systems. They also installed set-uid root shells to be used for easy root access.

III. Solution

A. Check your systems for signs of intrusion due to this incident.

1. Check the su, ftpd, and ftp binaries (for example, "/bin/su", "/usr/ucb/ftp" and "/usr/etc/in.ftpd" on Sun systems) against copies from distribution media.
2. Check for the presence of any of the following files:
   "/usr/etc/..." (dot dot dot), "/var/crash/..." (dot dot dot), "/usr/etc/.getwd", "/var/crash/.getwd", or "/usr/kvm/..." (dot dot dot).
3. Check for the presence of "+" in the "/etc/hosts.equiv" file.
4. Check the home directory for each entry in the "/etc/passwd" file for the presence of a ".rhosts" file containing "+ +" (plus space plus).
5. Search the system for the presence of the following set-uid root files: "wtrunc" and ".a".
6. Check for the presence of the set-uid root file "/usr/lib/lpx".

B. Take the following steps to secure your systems.

1. Save copies of the identified files to removable media.
2. Replace any modified binaries with copies from distribution media.
3. Remove the "+" entry from the "/etc/hosts.equiv" file and the "+ +" (plus space plus) entry from any ".rhosts" files.
4. Remove any of the set-uid root files that you find, which are mentioned in A5 or A6 above.
5. Change every password on the system.
6. Inspect the files mentioned in A2 above for references to other hosts.

This document is available from: http://www. cert.org/advisories/CA-1992-03.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached Copyright Statement
```

4 CA-1992-04: AT&T /usr/etc/rexecd Vulnerability

Original issue date: February 25, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in AT&T TCP/IP Release 4.0 running on SVR4 systems for both the 386/486 and 3B2 RISC platforms.

The existing error, in the remote execution server /usr/etc/rexecd, has been corrected, and a new executable for rexecd is available from AT&T by calling 800-543-9935. Patches may be obtained outside the U.S. by calling your local technical support. The numbers associated with the fix are 5127 (3.5" media) and 5128 (5.25" media).

The problem does not exist in TCP/IP release 3.2 for SVR3, or any earlier versions of the TCP/IP product running on either the 3B2 or 386 platforms.

The version of TCP/IP distributed with SVR4 by UNIX(r) System Laboratories, Inc. (a subsidiary of AT&T) does not contain this vulnerability.

UNIX(r) is a registered trademark of UNIX System Laboratories, Inc.

I. Description

A vulnerability has been identified where root privileges may be accessed through the use of /usr/etc/rexecd.

II. Impact

A user on a remote machine may be able to run commands as root on the target host (the host running the affected /usr/etc/rexecd).

III. Solution

1. Administrators of affected systems should execute, as root, the following command to immediately turn off access to rexecd until the new binary can be obtained.

   ```
   # chmod 400 /usr/etc/rexecd
   ```
2. Obtain and install the new patch. The fix will be supplied as one diskette, and it comes with one page of instructions documenting the procedure to replace the existing /usr/etc/rexecd binary.

The CERT/CC wishes to thank Bradley E. Smith, Network & Technical Services, Bradley University, for bringing this vulnerability to our attention and for providing a corresponding solution. We would also like to thank AT&T for their very quick response to this problem.

This document is available from: http://www. cert.org/advisories/CA-1992-04.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached Copyright Statement
```

5 CA-1992-05: AIX REXD Daemon Vulnerability

Original issue date: March 5, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability with the rexd daemon in versions 3.1 and 3.2 of AIX for IBM RS/6000 machines.

IBM is aware of the problem and it will be fixed in future updates to AIX 3.1 and 3.2. Sites may call IBM Support (800-237-5511) and ask for the patch for apar ix21353. Patches may be obtained outside the U.S. by contacting your local IBM representative.

The fix is also provided below.

I. Description

In certain configurations, particularly if NFS is installed, the rexd (RPC remote program execution) daemon is enabled.

Note: Installing NFS with the current versions of "mknfs" will re-enable rexd even if it was previously disabled.

II. Impact

If a system allows rexd connections, anyone on the Internet can gain access to the system as a user other than root.

III. Solution

CERT/CC and IBM recommend that sites take the following actions immediately. These steps should also be taken whenever "mknfs" is run.

1. Be sure the rexd line in /etc/inetd.conf is commented out by having a '#' at the beginning of the line:
   ```
   #rexd   sunrpc_tcp tcp  wait  root  /usr/etc/rpc.rexd rexd 100017
   1
   ```
2. Refresh inetd by running the following command as root:
   ```
   refresh -s inetd
   ```

The CERT/CC wishes to thank Darren Reed of the Australian National University for bringing this vulnerability to our attention and IBM for their response to the problem.

This document is available from: http://www. cert.org/advisories/CA-1992-05.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

6 CA-1992-06: AIX uucp Vulnerability

Original issue date: March 19,1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability with the UUCP software in versions of AIX up to 2007. The vulnerability does not exist in AIX 3.2.

IBM is aware of this problem, and a fix is available as apar number "ix18516". This patch is available for all AIX releases from GOLD to 2006.

The fix is in the 2007 update and 3.2 release of AIX. IBM customers may call IBM Support (800-237-5511) and ask that the fix be shipped to them. Patches may be obtained outside the U.S. by contacting your local IBM representative.

I. Description

Previous versions, except AIX 3.2, of the UUCP software contained incorrectly configured versions of various files.

II. Impact

Local users can execute unauthorized commands and gain unauthorized root access.

III. Solution

If allowing users access to the uucp isn't necessary, disable it.

```
% chmod 0100 /usr/bin/uucp
```

Obtain the fix from IBM Support. Install the fix following the instructions in the README file.

The CERT/CC would like to thank Steve Knodle, Clarkson University, for bringing this security vulnerability to our attention.

This document is available from: http://www. cert.org/advisories/CA-1992-06.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

7 CA-1992-07: AIX /bin/passwd Vulnerability

Original issue date: March 31, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability with the passwd command in AIX 3.2 and the 2007 update of AIX 3.1.

IBM is aware of this problem, and a fix is available as apar number "ix23505". Patches are available for AIX 3.2 and the 2007 update of AIX 3.1.

This fix may be ordered from Level 2 support or by anonymous ftp from software.watson.ibm.com (129.34.139.5) on the Internet.

To order from IBM call 1-800-237-5511 and ask that the fix be shipped. Patches may be obtained outside the U.S. by contacting your local IBM representative. If you are on the Internet, use anonymous ftp to obtain the fix from software.watson.ibm.com.

Patch	Filename	Checksum
AIX 3.2	pub/aix3/pas.32.tar.Z	54431 2262
AIX 3.1 2007	pub/aix3/pas.31.tar.Z	06703 99

Patches should be retrieved using binary mode.

IBM is currently incorporating the fix into the 3.2 version and 3.1 updates of AIX. Future shipments of these products should not be vulnerable to this problem. If you have any questions about products you receive, please contact your IBM representative.

I. Description

The passwd command contains a security vulnerability.

II. Impact

Local users can gain unauthorized root access.

III. Solution

A. As root, disable /bin/passwd until you obtain and install the patch.

```
# chmod 0500 /bin/passwd
```

B. Obtain the fix from IBM and install according to the directions provided with the patch.

The CERT/CC would like to thank Paul Selick of the University of Toronto for bringing this security vulnerability to our attention. We would also like to thank IBM for their quick response to this problem, and for making the patches available via anonymous ftp.

This document is available from: http://www. cert.org/advisories/CA-1992-07.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

8 CA-1992-08: Silicon Graphics Computer Systems IRIX lp Vulnerability

Original issue date: April 10, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a method of unauthorized root access in the lp software in Silicon Graphics Computer Systems (SGI) IRIX operating systems. This vulnerability is present in all current versions of IRIX.

Silicon Graphics Computer Systems and the CERT/CC strongly recommend that sites take immediate action to eliminate this vulnerability from their systems.

This vulnerability will be fixed in IRIX 4.0.5 and is NOT present in any version of the Trusted IRIX/B product.

I. Description

When IRIX pre-4.0.5 systems are installed or updated using either the basic system software ("eoe1.sw.unix") or the system manager software ("eoe2.sw.vadmin") media, a vulnerability is introduced in the lp software.

II. Impact

Any user logged into the system can gain root access.

III. Solution

As root, execute the following commands:

```
# cd /usr/lib
# chmod a-s,go-w lpshut lpmove accept reject lpadmin
# chmod go-ws lpsched vadmin/serial_ports vadmin/users vadmin/disks
# cd /usr/bin
# chmod a-s,go-w disable enable
# chmod go-ws cancel lp lpstat
```

If the eoe2.sw.vadmin software is not installed, you may ignore any warning messages from chmod such as:

"chmod: WARNING: can't access vadmin/serial_ports"

If system software should ever be reinstalled from pre-4.0.5 media or restored from a backup tape created before the patch was applied, repeat the above procedure before enabling logins by normal users.

The CERT/CC would like to thank Silicon Graphics Computer Systems for bringing this security vulnerability to our attention and for their quick response to this problem.

This document is available from: http://www. cert.org/advisories/CA-1992-08.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

9 CA-1992-09: AIX Anonymous FTP Vulnerability

Original issue date: April 27, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the anonymous FTP configuration in all versions of AIX.

IBM is aware of this problem and a fix is available as apar number "ix23944". This patch is available for all AIX releases from "GOLD".

IBM customers may call IBM Support (800-237-5511) and ask that the fix be shipped to them. Patches may be obtained outside the U.S. by contacting your local IBM representative. The fix will appear in the upcoming 2009 update and the next release of AIX.

I. Description

Previous versions of the anonymous FTP installation script, /usr/lpp/tcpip/samples/anon.ftp, incorrectly configured various files and directories.

II. Impact

Remote users can execute unauthorized commands and gain access to the system if anonymous FTP has been installed.

III. Solution

A. Obtain the fix from IBM Support.

The fix contains three files:

- a "readme" file (README.a23944),
- the fix installation script (install.a23944),
- and an archive containing the updated files (PATCH.a23944.Z).

B. Install the fix following the instructions in the README file.

The CERT/CC would like to thank Charles McGuire of the Computer Science Department, the University of Montana for bringing this security vulnerability to our attention and IBM for their response to the problem.

This document is available from: http://www. cert.org/advisories/CA-1992-09.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

10 CA-1992-10: AIX crontab Vulnerability

Original issue date: May 26, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in *crontab(1)* in version 3.2 of IBM's AIX operating system.

IBM is aware of this problem and a fix is available as apar number "ix26997" for AIX version 3.2. The version information for the patched /usr/bin/crontab is shown in the following *what(1)* output:

```
% what /usr/bin/crontab
04 1.23 com/cmd/cntl/cron/crontab.c, cmdcntl, bos320, 9218320f
4/8/92 11:50:42
07 1.8  com/cmd/cntl/cron/permit.c, bos, bos320 4/25/91 17:16:59
11 1.15  com/cmd/cntl/cron/cronsub.c, bos, bos320 8/18/91 20:42:32
06 1.9  com/cmd/cntl/cron/funcs.c, bos, bos320 6/8/91 21:22:40
```

If your crontab contains older modules than the above output indicates, we suggest that you install the fix.

I. Description

The distributed version of /usr/bin/crontab contains a security vulnerability.

II. Impact

Local users can gain unauthorized root access to the system.

III. Solution

The CERT/CC suggests that sites install the fix that IBM has made available. As an interim step, we suggests that sites prevent all non-root users from running /usr/bin/crontab by removing (or renaming) the /var/adm/cron/cron.allow and /var/adm/cron/cron.deny files.

- Obtain the fix from IBM Support.
    1. To order from IBM call 1-800-237-5511 and ask that the fix be shipped. Patches may be obtained outside the U.S. by contacting your local IBM representative.
    2. If you are on the Internet, use anonymous ftp to obtain the fix from software.watson.ibm.com (129.34.139.5).

Patch	Filename	Checksum
AIX 3.2	pub/aix3/cronta.tar.Z	02324 154

The patch must be retrieved using binary mode.

- Install the fix following the instructions in the README file.

The CERT/CC would like to thank Fuat Baran of Advanced Network & Services, Inc. for bringing this security vulnerability to our attention and IBM for their quick response to this problem.

This document is available from: http://www.cert.org/advisories/CA-1992-10.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

11 CA-1992-11: SunOS Environment Variables and setuid/setgid Vulnerability

Original issue date: May 27, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability involving environment variables and setuid/setgid programs under Sun Microsystems Computer Corporation SunOS. This vulnerability exists on all Sun architectures running SunOS 4.0 and higher.

In-house and third-party software can also be impacted by this vulnerability. For example, the current versions of rnews, sudo, smount, and npasswd are known to be vulnerable under SunOS. See the Description section of this advisory for details of how to identify software which may be vulnerable.

The workaround detailed in this advisory can be used to protect vulnerable software on SunOS operating system versions for which patches are unavailable, or for local or third party software which may be vulnerable.

Sun has provided patches for SunOS 4.1, 4.1.1, and 4.1.2 programs which are known to be impacted by this vulnerability. They are available through your local Sun Answer Center as well as through anonymous ftp from the ftp.uu.net (137.39.1.9) system in the /systems/sun/sun-dist directory.

Fix	PatchID	Filename	Checksum
login and su	100630-01	100630-01.tar.Z	36269 39
sendmail	100377-04	100377-04.tar.Z	14692 311

Note: PatchID 100630-01 contains the international version of /usr/bin/login. PatchID 100631-01 contains the domestic version of /usr/bin/login and is only available from Sun Answer Centers for sites that use the US Encryption Kit.

Please note that Sun will occasionally update patch files. If you find that the checksum is different please contact Sun or the CERT/CC for verification.

I. Description

A security vulnerability exists if a set-user-id program changes its real and effective user ids to be the same (but not to the invoker's id), and subsequently causes a dynamically-linked program to be exec'd. A similar vulnerability exists for set-group-id programs.

In particular, SunOS /usr/lib/sendmail, /usr/bin/login, /usr/bin/su, and /usr/5bin/su are vulnerable to this problem.

II. Impact

Local users can gain unauthorized privileged access to the system.

III. Solution

A. Obtain and install the patches from Sun or from ftp.uu.net following the provided instructions.

B. The following workaround can be used to protect vulnerable binaries for which patches are unavailable for your SunOS version, or for local or third party software which may be vulnerable.

The example given is a workaround for /usr/lib/sendmail.

1. As root, rename the existing version of /usr/lib/sendmail and modify the permissions to prevent misuse.

```
            # mv /usr/lib/sendmail /usr/lib/sendmail.dist
            # chmod 755 /usr/lib/sendmail.dist
```

2. In an empty temporary directory, create a file wrapper.c containing the following C program source (remember to strip any leading white-space characters from the #define lines).

```
/* Start of C program source */
/* Change the next line to reflect the full pathname of the file
to be protected by the wrapper code   */
            #define COMMAND "/usr/lib/sendmail.dist"
            #define VAR_NAME "LD_"
            main(argc,argv,envp)
            int argc;
            char **argv;
            char **envp;
            {
                  register char  **cpp;
                  register char  **xpp;
register char   *cp;
                  for (cpp = envp; cp = *cpp;) {
if (strncmp(cp, VAR_NAME, strlen(VAR_NAME))==0) {
for (xpp = cpp; xpp[0] = xpp[1]; xpp++);
                                    /* void */ ;
                              }
                              ee {

                                     cpp++;

                             }

}
```

```
                    execv(COMMAND, argv);

                    perror(COMMAND);

                    exit(1);

            }

   /* End of C program source */
```

3. As root, compile the C program source for the wrapper and install the resulting binary.

   ```
           # make wrapper
           # mv ./wrapper /usr/lib/sendmail
           # chown root /usr/lib/sendmail
           # chmod 4711 /usr/lib/sendmail
   ```

4. Steps 1 through 3 should be repeated for other vulnerable programs with the appropriate substitution of pathnames and file names. The "COMMAND" C preprocessor variable within the C program source should also be changed to reflect the appropriate renamed system binary.

The CERT/CC wishes to thank the following for their assistance: CIAC, PCERT, and in particular Wietse Venema of Eindhoven University, The Netherlands, for his support in the analysis of and a workaround for this problem. We also wish to thank Sun Microsystems Computer Corporation for their prompt response to this vulnerability.

This document is available from: http://www. cert.org/advisories/CA-1992-11.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

12 CA-1992-12: Revised SunOS rpc mountd Vulnerability

Original issue date: May 28, 1992

**** Superseded by CA-1994-02. ****

13 CA-1992-13: SunOS NIS Vulnerability

Original issue date: June 4, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning several vulnerabilities with NIS under Sun Microsystems, Inc. SunOS. These vulnerabilities exist in NIS under SunOS 4.1, 4.1.1, and 4.1.2, and may or may not exist in earlier versions of NIS.

Sun has provided fixes for SunOS 4.1, 4.1.1, and 4.1.2 for these vulnerabilities. The patch file containing these fixes is available through your local Sun Answer Center and through anonymous ftp from ftp.uu.net (137.39.1.9) in the /systems/sun/sun-dist directory. Note that these fixes will probably not be compatible with SunOS 4.0.3 and earlier versions of the operating system.

Fix	PatchID	Filename	Checksum
/usr/etc/{ypserv,ypxfrd,portmap}	100482-2	100482-02.tar.Z	53416 284

Please note that Sun will occasionally update patch files. If you find that the checksum is different, please contact Sun or the CERT/CC for verification.

I. Description

A security vulnerability exists under NIS allowing unauthorized access to NIS information.

II. Impact

A user on a remote host can obtain copies of the NIS maps from a system running NIS. The remote user can attempt to guess passwords for the system using the obtained NIS password map information.

III. Solution

A. Obtain and install the patch from Sun or from ftp.uu.net following the instructions provided in the "README" file.

1. As root, rename the existing versions of /usr/etc/{ypserv,ypxfrd,portmap} and modify the permissions to prevent misuse.

```
# mv /usr/etc/ypserv /usr/etc/ypserv.orig
# mv /usr/etc/ypxfrd /usr/etc/ypxfrd.orig
# mv /usr/etc/portmap /usr/etc/portmap.orig
```

```
        # chmod 0400 /usr/etc/ypserv.orig
        # chmod 0400 /usr/etc/ypxfrd.orig
# chmod 0400 /usr/etc/portmap.orig
```

2. Copy the new binaries into the /usr/etc directory.

```
        # cp `arch`/{4.1, 4.1.1, 4.1.2}/ypserv /usr/etc/ypserv
# cp `arch`/{4.1, 4.1.1, 4.1.2}/ypxfrd /usr/etc/ypxfrd
# cp `arch`/{4.1, 4.1.1, 4.1.2}/portmap /usr/etc/portmap
# chown root /usr/etc/ypserv /usr/etc/ypxfrd /usr/etc/portmap
# chmod 755 /usr/etc/ypserv /usr/etc/ypxfrd /usr/etc/portmap
```

3. Copy the securenets file to the /var/yp directory. Any site that has an existing /var/yp/securenets file should rename it prior copying the new version of the file.

```
# cp `arch`/{4.1, 4.1.1, 4.1.2}/securenets /var/yp
# chown root /var/yp/securenets
# chmod 644 /var/yp/securenets
```

4. Edit the /var/yp/securenets file to reflect the correct configuration for your site.

See the "README" file for details of the file syntax and special instructions for hosts with multiple Ethernet interfaces. The file should not contain any blank lines.

5. Reboot the system to invoke the new binaries.

The CERT/CC would like to thank Casper Dik of the University of Amsterdam, The Netherlands, and Peter Lamb of the Division of Information Technology, Commonwealth Scientific and Industrial Research Organization, Australia, for their assistance. We also wish to thank Sun Microsystems, Inc. for their response to this vulnerability.

This document is available from: http://www. cert.org/advisories/CA-1992-13.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

14 CA-1992-14: Altered System Binaries Incident

Original issue date: June 22, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information regarding a series of significant intrusion incidents on the Internet. Systems administrators should be aware that many systems on the Internet have been compromised due to this activity. To identify whether your systems have been affected by the activity we recommend that all system administrators check for the signs of intrusion detailed in this advisory.

This advisory describes the activities that have been identified as part of this particular incident. This does not address the possibility that systems may have been compromised due to other, unrelated intrusion activity.

I. Description

The intruders gain initial access to a host by discovering a password for a user account on the system, exploiting a "+" in the "/etc/hosts.equiv" file, or any ".rhosts" files on the system. The intruder then connects to the system using rsh and attempts to become root on the compromised system. An alias of "decode" may used to gain root privileges.

II. Impact

Having gained root access on a system, the intruders may make unauthorized changes to system binaries that can capture account information for both local and remote systems. In addition, the intruder adds "+ +" to any ".rhosts" files to which the intruder has access.

III. Solution

A. Check your systems for signs of intrusion due to this incident.

1. Check the login, telnet, and uucpd binaries (for example, "/bin/login", "/usr/ucb/telnet", and "/usr/etc/in.uucpd" on Sun systems) against copies from distribution media. Note that a check for creation or modification times and sizes is not sufficient to assure that the files have not been modified. The CERT/CC suggests that you compare the output of the "*sum(1)*" or "*cmp(1)*" command on both the distribution and installed versions of the binaries.
2. If the check from (A.1) indicates that your binaries have been modified, check for the presence of a password log file. Since the name of the logfile is often changed, the name of the file should be obtained using the "*strings(1)*" command on the Trojan login, uucpd, or telnet binary. Examples of filenames used on other systems are:

"/usr/spool/. " (dot space)
"/var/spool/secretmail/.l"
"/var/spool/secretmail/.log"
"/var/spool/secretmail/.tty"
"/var/spool/secretmail/.lock"
"/usr/tmp/.log"
"/usr/spool/uucp/.sys"
"/usr/spool/uucppublic/.hushlogin"
"/usr/uucp/.sys"
"/mnt2/lost+found/.tmp/.log"
"/usr/spool/mqueue/.AFG001"

Verify that the contents of files found using the "*strings(1)*" command do not contain valid username/password combinations.

3. Check for the presence of "+" in the "/etc/hosts.equiv" file.

   NOTE that Sun Microsystems installs the SunOS operating system with a default "+" in the /etc/hosts.equiv file for easy network access. This should be removed unless required in your operating environment and protected by a firewall network configuration. Leaving the "+" intact will allow any non-root user on the Internet to login to the system without a password.

4. Check the home directory for each entry in the "/etc/passwd" file for the presence of a ".rhosts" file containing "+ +" (plus space plus).

5. Assure that your "/etc/fstab", "/etc/inetd.conf", and "/etc/exports" files have not been modified.

B. Take the following steps to secure your systems.

1. Save copies of the identified files to removable media and remove any password log files as found in (A.2) above.
2. Replace any modified binaries with copies from distribution media.
3. Remove the "+" entry from the "/etc/hosts.equiv" file and the "+ +" (plus space plus) entry from any ".rhosts" files.
4. Change ownership of the "/etc" directory to userid "root" if it is owned by "bin" (as distributed by Sun).
5. Change every password on the system and assure that the new passwords are robust using a package such as Crack or Cops (available via anonymous ftp from cert.org).
6. Inspect and restore any changes made to your "/etc/fstab", "/etc/exports", or "/etc/inetd.conf" files. If any modifications are found in these files, you will need to unmount file systems and restart daemons once the files have been restored. Alternatively the system could be re-booted.
7. Remove the "decode" alias from your global mail aliases file ("/etc/aliases" on Sun systems, "/usr/lib/aliases" on other UNIX systems).

This document is available from: http://www. cert.org/advisories/CA-1992-14.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

15 CA-1992-15: Multiple SunOS Vulnerabilities Patched

Original issue date: July 21, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

*** This advisory supersedes CA-91.16. ***

The CERT/CC (Computer Emergency Response Team/Coordination Center) has received information concerning several vulnerabilities in the Sun Microsystems, Inc. (Sun) operating system (SunOS). These vulnerabilities affect all architectures and supported versions of SunOS including 4.1, 4.1.1, and 4.1.2 on sun3, sun3x, sun4, sun4c, and sun4m. The patches have been released as upgrades to three existing patch files.

Since application of these patches involves rebuilding your system kernel file (/vmunix), it is recommended that you apply all patches simultaneously. Use the procedure described below to apply the patches and rebuild the kernel.

Sun has provided patches for these vulnerabilities as updates to Patch IDs 100173, 100376, and 100567. They are available through your local Sun Answer Centers worldwide as well as through anonymous ftp from the ftp.uu.net (137.39.1.9) system (in the /systems/sun/sun-dist directory).

Fix	Patch ID	Filename	Checksum
NFS Jumbo	100173-08	100173-08.tar.Z	32716 562
Integer mul/div	100376-04	100376-04.tar.Z	12884 100
ICMP redirects	100567-02	100567-02.tar.Z	23118 13

Please note that Sun Microsystems sometimes updates patch files. If you find that the checksum is different please contact Sun Microsystems or CERT for verification.

NFS jumbo patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, all architectures

I. Description

The upgrade to the NFS Jumbo patch addresses a vulnerability that allows an intruder to become root using NFS. This vulnerability affects all architectures and supported versions of SunOS.

II. Impact

A remote user may exploit this vulnerability to gain root access.

III. Solution

Extract the new files to be installed in the kernel.

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

Integer mul/div patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, SPARC architectures

I. Description

The integer mul/div patch upgrade addresses an additional problem with the integer multiplication emulation code on SPARC architectures that allows an intruder to become root. This vulnerability affects SPARC architectures (sun4, sun4c, and sun4m) for all supported versions of SunOS (4.1, 4.1.1, and 4.1.2).

II. Impact

A local user may exploit a bug in the emulation routines to gain root access or crash the system.

III. Solution

Extract the new files to be installed in the kernel. Note that this patch applies only to SPARC architectures.

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

ICMP redirects patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, all architectures

I. Description

The ICMP redirects patch addresses a denial of service vulnerability with SunOS that allows an intruder to close existing network connections to and from a Sun system. This vulnerability affects all Sun architectures and supported versions of SunOS.

II. Impact

A remote user may deny network services on a Sun system.

III. Solution

Extract the new file to be installed in the kernel (the patch is the same for all supported versions of SunOS).

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

The CERT/CC wishes to thank Helen Rose of the EFF, Gordon Irlam of the University of Adelaide, Wietse Venema of Eindhoven University, and Ken Pon at Sun Microsystems, Inc for their assistance.

This document is available from: http://www. cert.org/advisories/CA-1992-15.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

16 CA-1992-16: VMS Monitor Vulnerability

Original issue date: September 22, 1992

**** Superseded by CA-1992-18. ****

17 CA-1992-17: HP NIS ypbind Vulnerability

Original issue date: October 5, 1992

**** Superseded by CA-1993-01. ****

18 CA-1992-18: Revised VMS Monitor Vulnerability

Original issue date: November 17,1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

***** THIS IS A REVISED CERT ADVISORY *****
***** IT CONTAINS NEW INFORMATION REGARDING AVAILABILITY OF IMAGE KITS *****
***** SUPERSEDES CERT ADVISORY CA-92.16 *****

The CERT Coordination Center received information concerning a potential vulnerability with Digital Equipment Corporation's VMS Monitor. This vulnerability is present in V5.0 through V5.4-2 but has been corrected in V5.4-3 through V5.5-1. The Software Security Response Team at Digital has provided the following information concerning this vulnerability.

The remedial image kit was not available at the time CERT distributed the CA-92.16.VMS.monitor.vulnerability advisory (dated September 22, 1992). At that time, Digital strongly suggested that customers either upgrade to VMS V5.4-3 (preferably to V5.5-1) or implement the provided workaround if unable to upgrade.

The following SSRT-200-1 addendum contains information about the availability of new images to address the possible vulnerability with VMS Monitor.

This last and final addendum includes new information about remedial images for VMS V5.0 through V5.4-2.

Digital strongly suggests that those customers who were unable to upgrade their systems (i.e., VMS V5.0 through V5.4-2) obtain and install the remedial image kit on their system(s).

For additional information, please contact your normal Digital Services Support Organization.

The information separated by the hard line is excerpted from the previously published CERT Advisory

SSRT-0200   PROBLEM: Potential Security Vulnerability Identified in Monitor

SOURCE: Digital Equipment Corporation

AUTHOR: Software Security Response Team - U.S.
Colorado Springs USA

PRODUCT: VMS

Symptoms Identified On: VMS, Versions 5.0, 5.0-1, 5.0-2, 5.1, 5.1-B, 5.1-1, 5.1-2, 5.2, 5.2-1, 5.3, 5.3-1, 5.3-2, 5.4, 5.4-1, 5.4-2

****

SOLUTION: This problem is not present in VMS V5.4-3
(released in October 1991) through V5.5-1
(released in July, 1992.)

****

PROBLEM/IMPACT:

Unauthorized privileges may be expanded to authorized users of a system under certain conditions, via the Monitor utility.   Should a system be compromised through unauthorized access, there is a risk of potential damage to a system environment. This problem will not permit unauthorized access entry, as individuals attempting to gain unauthorized access will continue to be denied through the standard VMS security mechanisms.

SOLUTION

This potential vulnerability does not exist in VMS V5.4-3 (released in October 1991) and later versions of VMS through V5.5-1. Digital strongly recommends that you upgrade to a minimum of VMS V5.4-3,and further, to the latest release of VMS V5.5-1. (released in July, 1992)

End of material excerpted from previously published CERT Advisory

Beginning of Text Provided by Digital Equipment Corporation

```
21-OCT-1992 SSRT-0200-1 (ADDENDUM)
21-AUG-1992 SSRT-0200
SOURCE:                Digital Equipment Corporation
AUTHOR:                Software Security Response Team - U.S.
                       Colorado Springs USA
PRODUCT: VMS MONITOR V5.0 through V5.4-2
PROBLEM:  Potential Security Vulnerability in VMS Monitor Utility
```

SOLUTION: A VMS V5.0 through V5.4-2 remedial kit is now available by contacting your normal Digital Services Support organization.

NOTE: This problem has been corrected in VAX VMS V5.4-3 (released in October 1991).

The kit may be identified as MONTOR$S01_05* or CSCPAT_1047 via DSIN, and DSNlink. Copyright (c) Digital Equipment Corporation, 1992 All Rights Reserved. Published Rights Reserved Under The Copyright Laws Of The United States.

ADVISORY ADDENDUM INFORMATION:

In August 1992, an advisory and article was distributed describing a potential security vulnerability discovered in the VMS Monitor utility and provided suggested workarounds to remove the vulnerability. The advisory was labeled SSRT-200 "Potential Security Vulnerability in VMS Monitor Utility".

This advisory follows that advisory with information of the availability of a kit containing a new sys$share:spishr.exe for VMS V5.0-* through VMS V5.4-2 and may be identified as MONTOR$S01_050 through MONTOR$S01_054 respectively from your Digital Services organization.

In the U.S.the kit is also identified as CSCPAT_1047 via DSIN and DSNlink.

Note:This potential vulnerability does not exist in VMS V5.4-3 and later versions of VMS. Digital strongly recommends that you upgrade to a minimum of VMS V5.4-3, and further, to the latest release of VMS V5.5-1. (released in July, 1992)

If you cannot upgrade to a minimum of VMS V5.4-3 at this time, Digital strongly recommends that you install the available V5.0-* through V5.4-2 kit on your system(s), available from your support organization, to avoid any potential vulnerability.

You may obtain a kit for VMS V5.0 through V5.4-2 by contacting your normal Digital Services support organization. (Customer Support Center, using DSNlink or DSIN, or your local support office)

As always, Digital recommends that you periodically review your system management and security procedures. Digital will continue to review and enhance the security features of its products and work with customers to maintain and improve the security and integrity of their systems.

End of Text provided by Digital Equipment Corporation

CERT wishes to thank Teun Nijssen of CERT-NL (the SURFnet CERT, in the Netherlands) for bringing this security vulnerability to our attention. We would also like to thank Digital Equipment Corporation's Software Security Response Team for providing information on this vulnerability.

This document is available from: http://www. cert.org/advisories/CA-1992-18.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

19 CA-1992-19: Keystroke Logging Banner

Original issue date: December 7, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information from the United States Department of Justice, General Litigation and Legal Advice Section, Criminal Division, regarding keystroke monitoring by computer systems administrators, as a method of protecting computer systems from unauthorized access.

The information that follows is based on the Justice Department's advice to all federal agencies. CERT strongly suggests adding a notice banner such as the one included below to all systems. Sites not covered by U.S. law should consult their legal counsel.

The legality of such monitoring is governed by 18 U.S.C. section 2510 et seq. That statute was last amended in 1986, years before the words "virus" and "worm" became part of our everyday vocabulary. Therefore, not surprisingly, the statute does not directly address the propriety of keystroke monitoring by system administrators.

Attorneys for the Department have engaged in a review of the statute and its legislative history. We believe that such keystroke monitoring of intruders may be defensible under the statute. However, the statute does not expressly authorize such monitoring. Moreover, no court has yet had an opportunity to rule on this issue. If the courts were to decide that such monitoring is improper, it would potentially give rise to both criminal and civil liability for system administrators. Therefore, absent clear guidance from the courts, we believe it is advisable for system administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to only authorized users will not be sufficient to place outside hackers on notice.

An agency's banner should give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring. The banner should also indicate to authorized users that they may be monitored during the effort to monitor the intruder (e.g., if a hacker is downloading a user's file, keystroke monitoring will intercept both the hacker's download command and the authorized user's file). We also understand that system administrators may in some cases monitor authorized users in the course of routine system maintenance. If this is the case, the banner should indicate this fact. An example of an appropriate banner might be as follows:

```
This system is for the use of authorized users only. Individu-
als using this computer system without authority, or in excess
```

> of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
>
> In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
>
> Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
>
> Each site using this suggested banner should tailor it to their precise needs. Any questions should be directed to your organization's legal counsel.

The CERT Coordination Center wishes to thank Robert S. Mueller, III, Scott Charney and Marty Stansell-Gamm from the United States Department of Justice for their help in preparing this Advisory.

This document is available from: http://www. cert.org/advisories/CA-1992-19.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

20 CA-1992-20: Cisco Access List Vulnerability

Original issue date: December 10,1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file. The CERT Coordination Center has received information concerning a vulnerability with Cisco routers when access lists are utilized. This vulnerability is present in Cisco software releases 8.2, 8.3, 9.0 and 9.1.

Systems and CERT strongly recommend that sites using Cisco routers for firewalls take immediate action to eliminate this vulnerability from their networks.

This vulnerability is fixed in Cisco software releases 8.3 (update 5.10), 9.0 (update 2.5), 9.1 (update 1.1) and in all later releases. Customers who are using software release 8.2 and do not want to upgrade to a later release should contact Cisco's Technical Assistance Center (TAC) at 800-553-2447 (Internet: tac@cisco.com) for more information.

The following interim releases are available via anonymous FTP from ftp.cisco.com (131.108.1.111).

Note: this FTP server will not allow filenames to be listed or matched with wildcards. You also cannot request the file by its full pathname. You must first cd to the desired directory (beta83_dir, beta90_dir, or beta91_dir) and then request the file desired (gs3-bfx.83-5.10, etc.).

Release (Update)	Filename	Size	Checksum
8.3 (5.10)	/beta83_dir/gs3-bfx.83-5.10	1234696	02465 1206
9.0 (2.5)	/beta90_dir/gs3-bfx.90-2.5	1705364	47092 1666
9.1 (1.1)	/beta91_dir/gs3-k.91-1.1	2005548	59407 1959

These releases are also available on Cisco's Customer Information On-Line (CIO) service for those customers having a maintenance contract. Other customers may obtain these releases through Cisco's Technical Assistance Center or by contacting their local Cisco distributor.

I. Description

A vulnerability in Cisco access lists allows some packets to be erroneously routed which one would expect to be filtered by the access list and vice-versa. This vulnerability can allow unauthorized traffic to pass through the gateway and can block authorized traffic.

II. Problem

If a Cisco router is configured to use extended IP access lists for traffic filtering on an MCI, SCI, cBus or cBusII interface, and the IP route cache is enabled, and the "established" keyword is used in the access list, then the access list can be improperly evaluated. This can permit packets which should be filtered and filter packets which should be permitted.

III. Workaround

This vulnerability can be avoided by either rewriting the extended access list to not use the "established" keyword, or by configuring the interface to not use the IP route cache. To disable the IP route cache, use the configuration command "no ip route-cache".

Example for a serial interface:

```
        router>enable
        Password:
        router#configure terminal
        Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
        interface serial 0
        no ip route-cache
        ^Z
        router#write memory
```

IV. Solution

Obtain and install the appropriate interim release listed above. Sites which are not experienced at this installation process should contact the TAC center at 800-553-2447 for assistance.

The CERT Coordination Center wishes to thank Keith Reynolds of the Santa Cruz Operation for his assistance in identifying this problem and Cisco Systems for their assistance in providing technical information for this advisory.

This document is available from: http://www. cert.org/advisories/CA-1992-20.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached copyright statement
```

21 CA-1992-21: Convex CSM: migmgr patch

Original issue date: December 16, 1992
Last revised: September 19, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The CERT Coordination Center has received information concerning several vulnerabilities in the following CONVEX Computer Corporation products: ConvexOS/Secure, CONVEX CXbatch, CONVEX Storage Manager (CSM), and ConvexOS EMACS. These vulnerabilities can affect ConvexOS versions V6.2 - V10.2 and ConvexOS/Secure versions V9.5 and V10.0 on all supported architectures.

CONVEX is aware of the vulnerabilities, and fixes or workarounds are available. Three of the fixes are implemented as full Engineering Change Notice (ECN) patches and, as such, will be shipped with all new systems as well as being released as upgrades for the products CXbatch, CSM and ConvexOS/Secure. There is a workaround available for the ConvexOS EMACS vulnerability. CONVEX is currently incorporating the fixes to these vulnerabilities into future releases of each product. Future shipments of these products should not be vulnerable to these problems.

If you have any questions about the affected products, please contact your CONVEX representative or the CONVEX Technical Assistance Center (TAC) at 1-800-952-0379.

ConvexOS/Secure: passwd patch

I. Description

The "passwd" command in ConvexOS/Secure contains a security vulnerability in versions V9.5 and V10.0 of ConvexOS/Secure. This vulnerability has been fixed in ConvexOS/Secure V10.1.

II. Impact

Local users can gain unauthorized root access.

III. Solution

Obtain and install ConvexOS/Secure V10.0.2 - Part No. 710-007815-008.

Convex CXbatch: qmgr patch

I. Description

The "qmgr" command in CONVEX CXbatch versions V1.0 - V2.1.3 contains a security vulnerability. This vulnerability is present in ConvexOS V6.2 - V10.2 on systems that have installed the optional CXbatch facility.

II. Impact

Local users can gain unauthorized root access.

III. Solution

A. As root, rename the existing version of /usr/convex/qmgr and

modify the permission (from 6755 to 700) to prevent misuse.

```
# /bin/mv /usr/convex/qmgr /usr/convex/qmgr.orig
# /bin/chmod 700 /usr/convex/qmgr.orig
```

B. Next, obtain and install CONVEX CXbatch V2.1.4 - Part No. 710-007830-011.

Convex CSM: migmgr patch

I. Description

The "migmgr" command in CONVEX CSM contains a security vulnerability, in ConvexOS version V10.1 of systems that have installed the CSM facility. This vulnerability will be fixed in the next CSM release.

II. Impact

Local users can gain unauthorized root access.

III. Solution

A. As root, rename the existing version of /usr/csm/bin/migmgr and modify the permission (from 4755 to 700) to prevent misuse.

```
# /bin/mv /usr/csm/bin/migmgr /usr/csm/bin/migmgr.orig
# /bin/chmod 700 /usr/csm/bin/migmgr.orig
```

B. Next, obtain and install CONVEX CSM V1.0.1 - Part No. 710-011315-003

ConvexOS: EMACS editor workaround

I. Description

The EMACS Editor in ConvexOS contains a security vulnerability, in ConvexOS versions V9.0 - V10.2.

II. Impact

Local users can gain unauthorized access to /dev/kmem.

III. Solution

As root, remove the setgid bit from /usr/convex/emacs.

```
      # /bin/chmod 755 /usr/convex/emacs
```

The CERT Coordination Center wishes to thank the CONVEX Computer Corporation for their response to these problems. We would also like to thank Bob Vickers from the University of London Computer Centre, London, England, for reporting the CXbatch problem to us.

This document is available from: http://www. cert.org/advisories/CA-1992-21.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
September 19,1997  Attached Copyright Statement
```